## Remarks

Claims 1, 3, 14, 16, 42-45, 47, 48, 51-54, and 58 are pending in this application. Claims 1, 3, 14, 16, 47, 48, and 58 have been amended in various particulars as indicated hereinabove. Claims 5-13, 18-27, 29, 31-39, 56, 57, and 59 have been cancelled without prejudice or disclaimer.

Claims 1, 3, 5, 10-16, 18, 27, 29, 31, 36-39, 42, 43, 47, 51, 52, 56, and 58 were rejected under 35 U.S.C. 103(a) as being unpatentable over Malan *et al.* (US Pub. No. 2002/0032871, hereinafter "Malan") in view of Poletto *et al.* (US Pub. No. 2002/0032880, hereinafter "Poletto"), and further in view of Katoh *et al.* (US Patent No. 5,949,757, hereinafter "Katoh"). This rejection is respectfully traversed for the following reasons.

Independent claims 1 and 14 were amended to include subject matter based on previous claims 6 and 19.

Independent claim 58 was amended to include features similar to claim 48.

Thus, this rejection should be deemed overcome.

Claims 6-9, 19-26, and 32-35 were rejected under 35 U.S.C. 103(a) as being unpatentable over Malan *et al.* (US Pub. No. 2002/0032871) in view of Poletto *et al.* (US Pub. No. 2002/0032880), and further in view of Katoh *et al.* (US Patent No. 5,949,757) and Li (US Patent No. 5,473,599). This rejection is deemed moot in view of the cancellation of the underlying claims.

Nevertheless, please consider the following comments in the event that this rejection is deemed applicable to claims 1 and 14, as amended herein.

Claim 1, for example, concerns a network comprising a first network domain and two routing devices for routing traffic into and out of the domain. A monitor/regulator analyzes flow records received from the two routing devices to determine whether the domain is sourcing a denial of service attack. The monitor/regulator makes the

determination based at least in part on differential characteristics between request packets routed out of the first network domain and response packets routed into the first network domain and instructs the first routing device and the second routing device to lower a priority of the undesirable network traffic that is being sourced from the first network domain.

According to the claimed invention, the determination of whether the domain is sourcing undesirable traffic is made based on aggregated network traffic routed by the first routing device and the second routing device.

There are advantages to making the determination based on the aggregated information from both routers:

> By aggregating or otherwise takes into consideration characteristic data of network traffics sourced out of routing device **114"a** as well as routing device **114"b**, monitor/regulator **102"** is made more sensitive, and be able to detect undesirable/inappropriate network traffics being sourced out network domain **104"**, even though the decision metrics may not be exceeded at the individual boundary routing devices **114"a** and/or **114"b**.

See Application as filed at page 14.

As recognized by the pending Office Action, only the Li shows a two router system. In any event, the pending claims are directed to more than simply the concept of using to routers. Instead, the claims are directed to a system that determines whether a domain is sourcing undesirable traffic by monitoring two routers and further based on the aggregated network traffic routed by those routers.

This functionality is neither shown nor suggested by any of the applied references. Thus, the rejection should be withdrawn.

Claims 44 and 53 were rejected under 35 U.S.C. 103(a) as being unpatentable over Malan *et al.* (US Pub. No. 2002/0032871) in view of Poletto *et al.* (US Pub. No. 2002/0032880), and further in view of Katoh *et al.* (US Patent No. 5,949,757) and Carr (US Patent No. 5,283,379). Also, claims 45 and 54 were rejected under 35 U.S.C. 103(a) as being unpatentable over Malan *et al.* (US Pub. No. 2002/0032871) in view of Poletto *et al.* (US Pub. No. 2002/0032880,), and further in view of Katoh *et al.* (US Patent No. 5,949,757) and Galloway (US Patent No. 5,430,709).

These rejections are moot in view of the amendments to the base claims.

Claim 59 was rejected under 35 U.S.C. 103(a) as being unpatentable over Malan *et al.* (US Pub. No. 2002/0032871) in view of Poletto *et al.* (US Pub. No. 2002/0032880,), and further in view of Katoh *et al.* (US Patent No. 5,949,757) and Ko *et al.* (US Patent No. 6,789,202). This rejection is now moot in view of the cancellation of claim 59.

Claims 48 and 57 were rejected under 35 U.S.C. 103(a) as being unpatentable over Malan *et al.* (US Pub. No. 2002/0032871) in view of Ko *et al.* (US Patent No. 6,789,202). This rejection is respectfully traversed for the following reasons.

Claim 48 and claim 58, as amended, include the feature of, upon determining that undesirable network traffics are being sourced out of one network domain, lowering a threshold for concluding that undesirable network traffic are being sourced out of a different network domain.

The instant Application as filed enumerates the benefits of this feature at page 17:

devices and/or the individual network domains. For example, upon determining that undesirable network traffics are being sourced out of one domain, the threshold criteria for concluding that undesirable network traffics are being sourced out of another domain may be "lowered", as the probability of erroneously concluding that a domain is also being exploited to support the attack is substantially lower, given it has already been determined another domain is being exploited to source an attack. Accordingly, under this embodiment, the detection and prevention can advantageously leverage on information learned and/or determination made for other domains.

The assumption is that the timing of denial of service attacks are sometimes correlated. So if a network attack appears in one place, other attacks may also be occurring in other places.

The pending Office Action points to the Ko patent at columns 4 and 5 for this feature. Those portions of the Ko patent really relate to something very different, however.

The Ko patent describes a system in which "local analyzers" are installed on host computers and report back to global analyzer. In one application, these local analyzers report back on the number of "password tries" made on the host computer.

The functionality from the Ko patent bears no relationship to the present claimed invention. Whereas the present claimed invention concerns setting thresholds for denial of service attacks using information from routers on different network domains, Ko is merely concerned with obtaining information concerning password tries reported by host computers.

Thus, this rejection should also be withdrawn.

It is believed that the present application is in condition for allowance. A Notice of Allowance is respectfully solicited. Should any questions arise, the Examiner is encouraged to contact the undersigned.

Respectfully submitted,

By /grant houston/
J. Grant Houston
Registration No.: 35,900
Tel.: 781 863 9991
Fax: 781 863 9931

Lexington, Massachusetts 02421
Date: August 17, 2010